

On Two Conjectures about Permutation Trinomials over $\mathbb{F}_{3^{2k}}$

Nian Li *

Abstract

Permutation polynomials with few terms attracts researchers' interest in recent years due to their simple algebraic form and some additional extraordinary properties. In this paper, by analyzing the quadratic factors of a fifth-degree polynomial and a seventh-degree polynomial over the finite field $\mathbb{F}_{3^{2k}}$, two conjectures on permutation trinomials over $\mathbb{F}_{3^{2k}}$ proposed recently by Li, Qu, Li and Fu are settled, where k is a positive integer.

1 Introduction

A permutation polynomial over a finite field is a polynomial that acts as a permutation of the elements of the field. Permutation polynomials were first studied by Hermite [6] for prime fields and by Dickson [3] for arbitrary finite fields. Permutation polynomials over finite fields have wide applications in coding theory, cryptography and combinatorial designs, and it is of great interest in both theoretical and practical aspects to find new permutation polynomials. The reader is referred to [1, 5, 8, 9, 10, 11, 18, 19, 20, 21, 23, 24, 25, 26] for some constructions of permutation polynomials over finite fields.

Let p be a prime, m be a positive integer and \mathbb{F}_{p^m} denote the finite field with p^m elements. An important class of permutation polynomials over the finite field \mathbb{F}_{p^m} is of the form

$$x^r h(x^{\frac{p^m-1}{d}}), \quad (1)$$

where r, d are positive integers satisfying $d \mid p^m - 1$, $1 \leq r < (p^m - 1)/d$ and $h(x) \in \mathbb{F}_{p^m}[x]$. This class of permutation polynomials originated from the work of Dickson [4], Carlitz and Wells [2] and Niederreiter and Robinson [16] who considered some special cases of the form (1). Wan and Lidl [22] first provided a unified criterion for a polynomial with the form (1) to be a permutation polynomial in terms of the primitive roots. Later, Park and Lee [17] and Zieve [27] studied this class of permutation polynomials and showed that the polynomial with the form (1) is a permutation polynomial if and only if $\gcd(r, (p^m - 1)/d) = 1$ and $x^r h(x)^{(p^m-1)/d}$ permutes the set μ_d of the d -th roots of unity in

*Department of Informatics, University of Bergen, N-5020 Bergen, Norway. Email: Nian.Li@uib.no

\mathbb{F}_{p^m} . In this sense, to determine the permutation property of (1), the crucial step is to decide whether $x^r h(x)^{(p^m-1)/d}$ permutes μ_d . However, this is still a difficult problem in general.

The construction of permutation trinomials with the form (1) reattracts researchers' attention due to a recent work of Ding et al [5]. Motivated by Ding et al.'s work, some new permutation trinomials of the form (1) were obtained in [7, 11, 12, 13] by using different approaches in solving equations with low degree over finite fields and in [14] by using the property of the linear fractional polynomials over finite fields. The results obtained in [14] are the generalizations of some works in [5, 7, 11, 12]. In a very recent paper [12], Li et al. constructed several classes of permutation trinomials of the form (1) with $m = 2k$ and $d = p^k + 1$ for $p = 2, 3$ and proposed three conjectures on permutation trinomials in such form for $p = 3$. This paper is devoted to settle two of the conjectures proposed in [12]. The key step to solve the conjectures is to prove that a fifth-degree equation and a seventh-degree equation over $\mathbb{F}_{3^{2k}}$ have a unique solution in μ_{3^k+1} , i.e., the set of the $(3^k + 1)$ -th roots of unity in $\mathbb{F}_{3^{2k}}$. By analyzing the quadratic factors of the corresponding fifth-degree and seventh-degree polynomials over $\mathbb{F}_{3^{2k}}$, we can obtain their possible quadratic factors and then the conjectures can be settled based on further discussions on the solutions to the quadratic factors.

The remainder of this paper is organized as follows. Section 2 introduces some notations and the conjectures proposed in [12]. Sections 3 and 4 prove two of the conjectures by analyzing the quadratic factors of a fifth-degree polynomial and a seventh-degree polynomial over $\mathbb{F}_{3^{2k}}$ respectively, and some concluding remarks are given in Section 5.

2 The two conjectures on permutation trinomials over $\mathbb{F}_{3^{2k}}$

Let p be a prime and m be a positive integer. A criterion for a polynomial in the form (1) to be a permutation polynomial had been characterized by the following lemma which was proved by Park and Lee in 2001 and reproved by Zieve in 2009.

Lemma 1. ([17, 27]) The polynomial defined as in (1) is a permutation over \mathbb{F}_{p^m} if and only if

- (1) $\gcd(r, (p^m - 1)/d) = 1$, and
- (2) $x^r h(x)^{(p^m-1)/d}$ permutes the set of the d -th roots of unity in \mathbb{F}_{p^m} .

Lemma 1 reduces the problem of determination of permutations over \mathbb{F}_{p^m} to that of determination of permutations over its subgroups. However, it is still a difficult problem to verify the second condition in Lemma 1. By using Lemma 1, Li, Qu, Li and Fu presented several classes of permutation trinomials of the form (1) with $m = 2k$ and $d = p^k + 1$ for $p = 2, 3$ by solving certain low-degree equations over finite fields and finally they proposed three conjectures on permutation trinomials over $\mathbb{F}_{3^{2k}}$.

From now on, let $m = 2k$ be a positive integer and $q = 3^k$. The set of the $(q + 1)$ -th roots of unity in \mathbb{F}_{q^2} is given as follows:

$$\mu_{q+1} = \{x \in \mathbb{F}_{q^2} : x^{q+1} = 1\}.$$

Conjecture 1. (Conjecture 5.1, [12])

- (1) Let $q = 3^k$, k be even and $f(x) = x^{lq+l+5} + x^{(l+5)q+l} - x^{(l-1)q+l+6}$, where $\gcd(5 + 2l, q - 1) = 1$. Then $f(x)$ is a permutation trinomial over \mathbb{F}_{q^2} .
- (2) Let $q = 3^k$, $f(x) = x^{lq+l+1} - x^{(l+4)q+l-3} + x^{(l-2)q+l+3}$ and $\gcd(1 + 2l, q - 1) = 1$. Then $f(x)$ is a permutation trinomial over \mathbb{F}_{q^2} .
- (3) Let $q = 3^k$, $f(x) = x^{lq+l+1} + x^{(l+2)q+l-1} - x^{(l-2)q+l+3}$ and $\gcd(1 + 2l, q - 1) = 1$. Then $f(x)$ is a permutation trinomial over \mathbb{F}_{q^2} if $k \not\equiv 2 \pmod{4}$.

According to Lemma 1, Conjecture 1 is equivalent to the following conjecture.

Conjecture 2. (Conjecture 5.2, [12])

- (1) Let $q = 3^k$, k be even and $g(x) = \frac{-x^7+x^6+x}{x^6+x-1}$. Then $g(x)$ permutes μ_{q+1} .
- (2) Let $q = 3^k$ and $g(x) = \frac{x^6+x^4-1}{-x^7+x^3+x}$. Then $g(x)$ permutes μ_{q+1} .
- (3) Let $q = 3^k$ and $g(x) = \frac{-x^5+x^3+x}{x^4+x^2-1}$. Then $g(x)$ permutes μ_{q+1} if $k \not\equiv 2 \pmod{4}$.

To prove Conjecture 2, we need to show that for any $g(x)$ listed above the equation $g(x) = t$ has a unique solution in μ_{q+1} for any $t \in \mu_{q+1}$. Normally, it is a hard problem to determine the number of solutions to an equation (even with low degree) over finite fields. As pointed out by the authors in [12], the main difficulty to prove these conjectures lies in dealing with some specified equations with high degree. In what follows, we aim to settle Conjecture 2 (2) and Conjecture 2 (3), for this goal we determine the quadratic factors of a fifth-degree polynomial and a seventh-degree polynomial and then show that $g(x) = t$ cannot have distinct solutions in μ_{q+1} respectively.

3 Proof of Conjecture 2 (3)

To prove Conjecture 2 (3), we first show that $x^4 + x^2 - 1 = 0$ has no solution in μ_{q+1} . Otherwise, we have $x^{q+1} = 1 = x^4 + x^2$ which implies that $x^q = x^3 + x$. Taking q -th power on both sides gives $x = x^{3q} + x^q = x^{-3} + x^{-1}$ which leads to $x^4 - x^2 - 1 = 0$, a contradiction with $x^4 + x^2 - 1 = 0$ and $x \in \mu_{q+1}$. On the other hand, it can be readily verified that $g(x)^{q+1} = 1$ for any $x \in \mu_{q+1}$. Thus, to prove Conjecture 2 (3), it suffices to show that $\frac{-x^5+x^3+x}{x^4+x^2-1} = t$ has a unique solution in μ_{q+1} for any $t \in \mu_{q+1}$ if $k \not\equiv 2 \pmod{4}$, which is equivalent to proving that the equation

$$x^5 + tx^4 - x^3 + tx^2 - x - t = 0 \tag{2}$$

has at most one solution in μ_{q+1} for any $t \in \mu_{q+1}$ if $k \not\equiv 2 \pmod{4}$.

Lemma 2. Let $t \in \mu_{q+1}$ and $F(x) = x^5 + tx^4 - x^3 + tx^2 - x - t$. If $x^2 + ax + b$, where $a, b \neq 0$, is a quadratic factor of $F(x)$, then a, b must satisfy $a^2 = (\epsilon - 1)b^2 - (\epsilon + 1)b + \epsilon - 1$, where $\epsilon^2 + 1 = 0$.

Proof. Assume that $F(x)$ can be factorized as $F(x) = (x^2 + ax + b)(x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3)$. Expanding the right hand side of $F(x)$ and comparing the coefficients of x^{4-i} for $i = 0, 1, \dots, 4$ gives

$$a + \sigma_1 = t, \quad b + \sigma_2 + a\sigma_1 = -1, \quad b\sigma_1 + a\sigma_2 + \sigma_3 = t, \quad a\sigma_3 + b\sigma_2 = -1, \quad b\sigma_3 = -t. \quad (3)$$

From the first two identities in (3) we have $b + \sigma_2 + a(t - a) = -1$ and then $\sigma_2 = a^2 - at - b - 1$, and by the last two identities in (3) we have $a(-t/b) + b\sigma_2 = -1$ which leads to $\sigma_2 = (at - b)/b^2$. This implies that $a^2 - at - b - 1 = (at - b)/b^2$, i.e.,

$$(a + ab^2)t = a^2b^2 - b^3 - b^2 + b. \quad (4)$$

On the other hand, by the third identity in (3) we have $b^2\sigma_1 + ab\sigma_2 + b\sigma_3 = bt$ which implies that $b^2(t - a) + a(-1 - a\sigma_3) + (-t) = bt$. Replacing σ_3 by $(-t/b)$ gives $b^3t - b^3a - ab + a^2t - bt = b^2t$, then we obtain that

$$(b^3 - b^2 - b + a^2)t = ab^3 + ab. \quad (5)$$

We then can discuss the relation between a and b as follows:

Case 1: $a + ab^2 = 0$. If this case happens, then we have $b^2 = -1$ since $a, b \neq 0$ and then (4) implies $a^2b^2 - b^3 - b^2 + b = 0$ which leads to $a^2b^2 - b(b^2 - 1) - b^2 = 0$, i.e., $a^2 = 1 - b$. By $b^2 = -1$ we have $ab^3 + ab = 0$ and then $b^3 - b^2 - b + a^2 = 0$ due to (5), i.e., $a^2 = b^2 + b(1 - b^2) = -1 - b$, a contradiction with $a^2 = 1 - b$. Thus, this case cannot happen.

Case 2: $b^3 - b^2 - b + a^2 = 0$. For this case, we then have $ab^3 + ab = 0$ according to (5), i.e., $b^2 = -1$ since $a, b \neq 0$ and then from $b^3 - b^2 - b + a^2 = 0$ we have $a^2 = b^2 + b(1 - b^2) = -1 - b$. Again by $b^2 = -1$ we can obtain $a + ab^2 = 0$ which leads to $a^2b^2 - b^3 - b^2 + b = 0$ by (4), i.e., $a^2 = 1 - b$, a contradiction with $a^2 = -1 - b$. Thus, this case cannot happen either.

Case 3: $a + ab^2 \neq 0$ and $b^3 - b^2 - b + a^2 \neq 0$. In this case, by (4) and (5) we have

$$\frac{a^2b^2 - b^3 - b^2 + b}{a + ab^2} = \frac{ab^3 + ab}{b^3 - b^2 - b + a^2}$$

which is equivalent to

$$a^4 - (b - 1)^2a^2 - (b^4 + 1) = 0$$

since $ab \neq 0$. Note that the discriminant of the above quadratic equation on variable a^2 is $\Delta = (b-1)^4 + 4(b^4 + 1) = -(b+1)^4$. This implies

$$a^2 = \frac{(b-1)^2 \pm \epsilon(b+1)^2}{2} = (-1 \pm \epsilon)b^2 + (-1 \mp \epsilon)b + (-1 \pm \epsilon),$$

where $\epsilon^2 + 1 = 0$. Then the result follows from $\epsilon^2 + 1 = (-\epsilon)^2 + 1 = 0$. This completes the proof. \square

Lemma 3. For any $t \in \mu_{q+1}$ (2) cannot have distinct solutions in μ_{q+1} if $k \not\equiv 2 \pmod{4}$.

Proof. Suppose that (2) have two distinct solutions $x_1, x_2 \in \mu_{q+1}$, this means that the polynomial $x^5 + tx^4 - x^3 + tx^2 - x - t$ has a quadratic factor $x^2 + ax + b$ satisfying $x_1 + x_2 = -a$ and $x_1x_2 = b$. Moreover, the two solutions can be expressed as

$$x_1 = a - \sqrt{a^2 - b}, \quad x_2 = a + \sqrt{a^2 - b}.$$

This together with Lemma 2 implies that

$$x_1 = a - \sqrt{\epsilon - 1}(b+1), \quad x_2 = a + \sqrt{\epsilon - 1}(b+1), \quad (6)$$

where $\epsilon^2 + 1 = 0$. Note that (2) has repeated roots if $b = -1$ and in this case the repeated root is $x = \epsilon$ according to Lemma 2. Next let $b \neq -1$ and α be a primitive element of \mathbb{F}_{q^2} , then $\epsilon = \pm \alpha^{(q^2-1)/4}$ and by $\epsilon^2 + 1 = 0$ we have $(\epsilon - 1)^2 = \epsilon$. Then we can discussion (6) as below:

- (1) $k \equiv 1, 3 \pmod{4}$. For this case, we can obtain that $q^2 - 1 \equiv 8 \pmod{16}$ which implies that $\sqrt{\epsilon - 1} \notin \mathbb{F}_{q^2}$ due to $(\epsilon - 1)^2 = \epsilon$. Thus (2) cannot have two distinct solutions in μ_{q+1} if $k \equiv 1, 3 \pmod{4}$.
- (2) $k \equiv 0 \pmod{4}$. In this case, by $x_1, x_2 \in \mu_{q+1}$, we have $(a \pm \sqrt{\epsilon - 1}(b+1))^{q+1} = 1$ which leads to

$$a^q \sqrt{\epsilon - 1}(b+1) + a \sqrt{\epsilon - 1}^q (b^q + 1) = 0. \quad (7)$$

On the other hand, according to $x_1 + x_2 = -a$ and $x_1x_2 = b$, we have $b \in \mu_{q+1}$ and $-a^q = x_1^q + x_2^q = (x_1 + x_2)/(x_1x_2) = -a/b$, i.e., $b^q = b^{-1}$ and $a^q = a/b$. Therefore, (7) can be reduced to $\sqrt{\epsilon - 1} + \sqrt{\epsilon - 1}^q = 0$ since $a, b, (b+1) \neq 0$. This is impossible since $\sqrt{\epsilon - 1}^{q-1} = (\sqrt{\epsilon - 1}^4)^{(q-1)/4} = \epsilon^{(q-1)/4} = (-1)^{(q-1)/8} = 1$ due to $(\epsilon - 1)^2 = \epsilon$ and $q - 1 \equiv 0 \pmod{16}$.

Combining the above cases, we can conclude that (2) cannot have distinct solutions in μ_{q+1} if $k \not\equiv 2 \pmod{4}$. This completes the proof. \square

According to Lemma 3, we complete the proof of Conjecture 2 (3). Next we prove Conjecture 2 (2) in the same manner by analyzing the quadratic factors of a seventh-degree polynomial over \mathbb{F}_{q^2} .

4 Proof of Conjecture 2 (2)

Notice that $-x^7 + x^3 + x \neq 0$ if $x \in \mu_{q+1}$. Otherwise we have $x^6 - x^2 = 1 = x^{q+1}$ and then $x^q = x^5 - x$. Taking q -th power on both sides gives $x = x^{5q} - x^q = x^{-5} - x^{-1}$ which leads to $x^6 + x^4 - 1 = 0$. This together with $x^6 - x^2 - 1 = 0$ gives $x^4 + x^2 = 0$, i.e., $x^2 = -1$, a contradiction. Thus, we have $-x^7 + x^3 + x \neq 0$ if $x \in \mu_{q+1}$. Then, for any $x \in \mu_{q+1}$, we have $g(x)^{q+1} = 1$, i.e., $g(x) \in \mu_{q+1}$. Therefore, to complete the proof of Conjecture 2 (2), it is sufficient to show that $\frac{x^6 + x^4 - 1}{-x^7 + x^3 + x} = \frac{1}{t}$ has a unique solution for any $t \in \mu_{q+1}$, i.e., the equation

$$x^7 + tx^6 + tx^4 - x^3 - x - t = 0 \quad (8)$$

has at most one solution in μ_{q+1} for any $t \in \mu_{q+1}$ for any positive integer k .

Similar as the proof of Conjecture 2 (3), we next show that (8) cannot have distinct solutions in μ_{q+1} for any $t \in \mu_{q+1}$ by analyzing the possible quadratic factors of $x^7 + tx^6 + tx^4 - x^3 - x - t$ over \mathbb{F}_{q^2} . Note that if (8) have distinct solutions in μ_{q+1} then $x^7 + tx^6 + tx^4 - x^3 - x - t$ must have a quadratic factor $x^2 + ax + b$ for some $a, b \in \mathbb{F}_{q^2}$ satisfying $a^q b = a$ according to the proof of Lemma 3.

Lemma 4. Let $t \in \mu_{q+1}$ and $G(x) = x^7 + tx^6 + tx^4 - x^3 - x - t$. If $x^2 + ax + b$, where $a, b \neq 0$ and $a^q b = a$, is a quadratic factor of $G(x)$, then a, b must satisfy one of the following conditions:

- (1) $(a, b) = (\epsilon, -1)$, where $\epsilon^2 + 1 = 0$.
- (2) $a^2 = \theta b^2 - (\theta - 1)b + \theta$, where $\theta^3 - \theta - 1 = 0$.

Proof. Assume that $G(x)$ can be factorized as $G(x) = (x^2 + ax + b)(x^5 + \sigma_1 x^4 + \sigma_2 x^3 + \sigma_3 x^2 + \sigma_4 x + \sigma_5)$. Expanding the right hand side of $G(x)$ and comparing the coefficients of x^{6-i} for $i = 0, 1, \dots, 6$ gives

$$a + \sigma_1 = t, \quad b + a\sigma_1 + \sigma_2 = 0, \quad b\sigma_1 + a\sigma_2 + \sigma_3 = t, \quad b\sigma_2 + a\sigma_3 + \sigma_4 = -1 \quad (9)$$

and

$$b\sigma_3 + a\sigma_4 + \sigma_5 = 0, \quad a\sigma_5 + b\sigma_4 = -1, \quad b\sigma_5 = -t. \quad (10)$$

By a direct calculation, from (9) we have $\sigma_1 = t - a$, $\sigma_2 = -a\sigma_1 - b = a^2 - at - b$, $\sigma_3 = t - a\sigma_2 - b\sigma_1 = t - a^3 + a^2t - bt - ab$ and $\sigma_4 = -1 - a\sigma_3 - b\sigma_2 = -1 - at + a^4 - a^3t - abt + b^2$. On the other hand, by (10), we can obtain $\sigma_5 = -t/b$, $\sigma_4 = (-1 - a\sigma_5)/b = (at - b)/b^2$ and $\sigma_3 = (-\sigma_5 - a\sigma_4)/b = (ab + bt - a^2t)/b^3$. Therefore, by the value of σ_3 we get $t - a^3 + a^2t - bt - ab = (ab + bt - a^2t)/b^3$, which can be written as

$$(a^2b^3 + a^2 - b^4 + b^3 - b)t = a^3b^3 + ab^4 + ab, \quad (11)$$

and according to the value of σ_4 we have $-1 - at + a^4 - a^3t - abt + b^2 = (at - b)/b^2$, i.e.,

$$(a + ab^2 + a^3b^2 + ab^3)t = a^4b^2 + b^4 - b^2 + b. \quad (12)$$

Then we can discuss (11) and (12) as follows:

Case 1: $a^2b^3 + a^2 - b^4 + b^3 - b = 0$. For this case, by (11) we have $a^3b^3 + ab^4 + ab = 0$, i.e., $a^2b^2 + b^3 + 1 = 0$ since $ab \neq 0$. Replacing b by a/a^q and then multiplying by a^{3q} gives $a^4a^q + (a+a^q)^3 = 0$, which leads to $a \in \mathbb{F}_q$ due to $aa^q, (a+a^q) \in \mathbb{F}_q$. Hence, again by $a^qb = a$ we get $b = 1$ and then $a^2 = 1$. This contracts with $a^2b^3 + a^2 - b^4 + b^3 - b = 0$. Thus this case cannot occur.

Case 2: $a+ab^2+a^3b^2+ab^3 = 0$, i.e., $a^2 = -(b^3+b^2+1)/b^2$. Then, (12) implies that $a^4b^2+b^4-b^2+b = 0$ which gives $a^4 = -(b^3-b+1)/b$. From these two identities one gets $(b^3+b^2+1)^2/b^4 = -(b^3-b+1)/b$, which can be reduced to $b^6+b^5+b^2-1 = 0$. Note that $b^6+b^5+b^2-1 = (b^6-1) + b^2(b^3+1) = (b^3+1)(b^3+b^2-1)$. Thus we get $b = -1$ or $b^3+b^2-1 = 0$. If $b = -1$, then $a^2 = -(b^3+b^2+1)/b^2 = -1$. If $b^3+b^2-1 = 0$, then $a^2 = -(b^3+b^2+1)/b^2 = 1/b^2$, which means $a^2 \in \mu_{q+1}$ since $b = a^{1-q} \in \mu_{q+1}$, i.e., $a^{2q+2} = 1$. Moreover, substituting $b = a^{1-q} \in \mu_{q+1}$ into $a^2b^2 = 1$ gives $a^{4-2q} = 1$, which leads to $a^{6-2q-2} = a^6 = (a^2)^3 = 1$. That is, $a^2 = 1$ and then $b^2 = 1$, a contradiction with $b^3+b^2-1 = 0$ due to $b \neq 0$. Hence, this case happens only if $a^2 = -1$ and $b = -1$.

Case 3: $a^2b^3 + a^2 - b^4 + b^3 - b \neq 0$ and $a + ab^2 + a^3b^2 + ab^3 \neq 0$. By (11) and (12), we have

$$\frac{a^3b^3 + ab^4 + ab}{a^2b^3 + a^2 - b^4 + b^3 - b} = \frac{a^4b^2 + b^4 - b^2 + b}{a + ab^2 + a^3b^2 + ab^3}$$

which can be reduced to $a^6 - (b+1)^4a^2 - (b^6 - b^5 - b^4 - b^2 - b + 1) = 0$ by a straight calculation since $ab \neq 0$. If $b = -1$, then we have $a^6 + 1 = (a^2 + 1)^3 = 0$, i.e., $a^2 = -1$. If $b \neq -1$, then the above equation can be rewritten as

$$\left(\frac{a^2}{(b+1)^2}\right)^3 - \frac{a^2}{(b+1)^2} - \frac{b^6 - b^5 - b^4 - b^2 - b + 1}{(b+1)^6} = 0.$$

Observe that $\frac{b^6 - b^5 - b^4 - b^2 - b + 1}{(b+1)^6} = \frac{b^6+1}{(b+1)^6} - \frac{b(b+1)^4}{(b+1)^6} = \frac{b^6+1}{(b+1)^6} - \frac{b}{(b+1)^2} = 1 + \frac{b^3}{(b+1)^6} - \frac{b}{(b+1)^2}$. Then, the above equation can be further written as

$$\left(\frac{a^2}{(b+1)^2} - \frac{b}{(b+1)^2}\right)^3 - \left(\frac{a^2}{(b+1)^2} - \frac{b}{(b+1)^2}\right) - 1 = 0,$$

which implies that $\frac{a^2}{(b+1)^2} - \frac{b}{(b+1)^2} = \theta$, i.e., $a^2 = \theta b^2 - (\theta - 1)b + \theta$, where $\theta^3 - \theta - 1 = 0$. This completes the proof. \square

According to Lemma 4, we can obtain the following desired result.

Lemma 5. For any $t \in \mu_{q+1}$ (8) cannot have distinct solutions in μ_{q+1} for any positive integer k .

Proof. Suppose that (8) have two distinct solutions $x_1, x_2 \in \mu_{q+1}$, then $x^7 + tx^6 + tx^4 - x^3 - x - t$ has a quadratic factor $x^2 + ax + b$ satisfying $x_1 + x_2 = -a$ and $x_1x_2 = b$ which implies $a^qb = a$. Moreover,

the two solutions can be expressed as

$$x_1 = a - \sqrt{a^2 - b}, \quad x_2 = a + \sqrt{a^2 - b}.$$

Note that $x_1 \neq x_2$ means $a^2 \neq b$ which indicates that the case $b = -1$ in Lemma 4 cannot occur. Then, by Lemma 4 (2), we can obtain

$$x_1 = a - \sqrt{\theta}(b+1), \quad x_2 = a + \sqrt{\theta}(b+1),$$

where $\theta^3 - \theta - 1 = 0$. Since $x^3 - x - 1$ is an irreducible polynomial over \mathbb{F}_3 , then by [15, Theorem 2.14] we have that $x^3 - x - 1 = 0$ has solutions in \mathbb{F}_{q^2} if and only if $2k \equiv 0 \pmod{3}$, i.e., $k \equiv 0 \pmod{3}$. Thus, if $k \not\equiv 0 \pmod{3}$, then the second case in Lemma 4 cannot occur and then (8) cannot have two distinct solutions in μ_{q+1} . Next we consider the case $k \equiv 0 \pmod{3}$. In this case, we have $\theta \in \mathbb{F}_{3^3} \subseteq \mathbb{F}_q$ due to [15, Theorem 2.14]. Moreover, by $\theta^3 - \theta - 1 = 0$, we have $\theta^{13} = \theta \cdot \theta^3 \cdot \theta^9 = \theta(\theta+1)(\theta-1) = \theta^3 - \theta = 1$. This implies that $\theta^{(q-1)/2} = 1$ since $q \equiv 1 \pmod{26}$ if $k \equiv 0 \pmod{3}$. On the other hand, by $x_1, x_2 \in \mu_{q+1}$, we have $(a \pm \sqrt{\theta}(b+1))^{q+1} = 1$ which leads to

$$a^q \sqrt{\theta}(b+1) + a \sqrt{\theta}^q (b^q + 1) = 0.$$

This together with $a^q = a/b$ and $b^q = 1/b$ gives $\sqrt{\theta} + \sqrt{\theta}^q = 0$, a contradiction with $\theta^{(q-1)/2} = 1$. Therefore, we can conclude that (8) cannot have two distinct solutions in μ_{q+1} for any positive integer k . This completes the proof. \square

Thus, we complete the proof of Conjecture 2 (2) according to Lemma 5.

To end this section, we point out that Conjecture 2 (1) can be discussed in the same way. To prove Conjecture 2 (1), we need to show that $\frac{-x^7+x^6+x}{x^6+x-1} = t$ has a unique solution for any $t \in \mu_{q+1}$. Similar to Lemma 4, by a direct calculation we can show that $x^7 + (t-1)x^6 + (t-1)x - t$ has a quadratic factor $x^2 + ax + b$, where $ab \neq 0$ and $a^q b = a$, only if a, b satisfy $a^6 + a^5 b + a^5 + a^4 b - a^3 b^2 - a^3 b - b^3 - 1 = 0$. Dividing a^6 on both sides gives $1 + (b+1)/a + b/a^2 - (b^2+b)/a^3 = (b+1)^6/a^6 - b^3/a^6$. Then, let $u = a^{-1} + a^{-q} = (b+1)/a$ and $v = a^{-1} \cdot a^{-q} = b/a^2$ we can get $v^3 - (u-1)v - (u^6 - u - 1) = 0$, i.e., $(v-1)^3 - (u-1)(v-1) - u^6 = 0$. However, currently we do not know how to use this identity to prove that $x^2 + ax + b = 0$ cannot have distinct solutions in μ_{q+1} for even k .

5 Conclusion remarks

In this paper, by analyzing the possible quadratic factors of a fifth-degree polynomial and a seventh-degree polynomial over $\mathbb{F}_{3^{2k}}$, two of the conjectures on permutation trinomials over $\mathbb{F}_{3^{2k}}$ proposed recently by Li, Qu, Li and Fu in [12] were settled.

Acknowledgements

This work was supported by the Norwegian Research Council.

References

- [1] C. Bracken, C.H. Tan and Y. Tan, Binomial differentially 4 uniform permutations with high non-linearity, *Finite Fields Appl.* 18(3)(2012), pp. 537-546.
- [2] L. Carlitz and C. Wells, The number of solutions of a special system of equations in a finite field, *Acta Arith.* 12 (1966), pp. 77-84.
- [3] L.E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. of Math.*, 11 (1896), pp. 65-120.
- [4] L.E. Dickson, *Linear Groups with an exposition of the Galois field theory*, Dover, New York, 1958.
- [5] C. Ding, L. Qu, Q. Wang, J. Yuan and P. Yuan, Permutation trinomials over finite fields with even characteristic, *SIAM J. Dis. Math.*, 29 (2015), pp. 79-92.
- [6] Ch. Hermite, Sur les fonctions de sept lettres, *C. R. Acad. Sci. Paris*, 57 (1863), pp. 750-757.
- [7] Rohit Gupta and R.K. Sharma, Some new classes of permutation trinomials over finite fields with even characteristic, *Finite Fields Appl.* 41 (2016), pp. 89-96.
- [8] X. Hou, A class of permutation trinomials over finite fields, *Acta Arith.* 162 (2014), pp. 51-64.
- [9] X. Hou, Permutation polynomials over finite fields—A survey of recent advances, *Finite Fields Appl.* 32 (2015), pp. 82-119.
- [10] X. Hou, Determination of a type of permutation trinomials over finite fields, II, *Finite Fields Appl.* 35 (2015), pp. 16-35.
- [11] K. Li, L. Qu and X. Chen, New classes of permutation binomials and permutation trinomials over finite fields, available online: <http://arxiv.org/pdf/1508.07590.pdf>.
- [12] K. Li, L. Qu, C. Li and S. Fu, New permutation trinomials constructed from fractional polynomials, available online: <https://arxiv.org/pdf/1605.06216v1.pdf>
- [13] N. Li and T. Helleseht, Several classes of permutation trinomials from Niho exponents, submitted.
- [14] N. Li and T. Helleseht, New permutation trinomials from Niho exponents over finite fields with even characteristic, available online: <http://arxiv.org/pdf/1606.03768v1.pdf>

- [15] R. Lidl and H. Niederreiter, Finite Fields, 2nd ed. Cambridge Univ. Press, Cambridge, 1997.
- [16] N. Niederreiter and K.H. Robinson, Complete mappings of finite fields, J. Austral. Math. Soc. 33 (1982), pp. 197-212.
- [17] Y.H. Park and J.B. Lee, Permutation polynomials and group permutation polynomials, Bull. Austral. Math. Soc. 63 (2001), pp. 67-74.
- [18] Z. Tu, X. Zeng and L. Hu, Several classes of complete permutation polynomials, Finite Fields and Appl., 25 (2014), pp. 182-193.
- [19] Z. Tu, X. Zeng, L. Hu and C. Li, A class of binomial permutation polynomials, available online: <http://arxiv.org/pdf/1310.0337v1.pdf>.
- [20] Z. Tu, X. Zeng and Y. Jiang, Two classes of permutation polynomials having the form $(x^{2^m} + x + \delta)^s + x$, Finite Fields Appl. 31(2015), pp. 12-24.
- [21] Z. Tu, X. Zeng, C. Li and T. Helleseeth, Permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ over the finite field $\mathbb{F}_{p^{2m}}$ of odd characteristic, Finite Fields Appl. 34(2015), pp. 20-35.
- [22] D. Wan and R. Lidl, Permutation polynomials of the form $x^r h(x^{(q-1)/d})$ and their group structure, Monatshefte. Math. 112 (1991), pp. 149-163.
- [23] X. Zeng, X. Zhu, and Lei Hu, Two new permutation polynomials with the form $(x^{2^k} + x + d)^s + x$ over \mathbb{F}_{2^n} . Appl. Algebra Eng. Commun. Comput. 21(2)(2010), pp. 145-150.
- [24] X. Zeng, S. Tian, and Z. Tu, Permutation polynomials from trace functions over finite fields, Finite Fields Appl. 35(2015), pp. 36-51.
- [25] X. Zhu, X. Zeng, and Y. Chen, Some binomial and trinomial differentially 4-uniform permutation polynomials, Int. J. Found. Comput. Sci. 26(4)(2015), pp. 487-498.
- [26] M. Zieve, Permutation polynomials on \mathbb{F}_q induced from Rédei function bijections on subgroups of \mathbb{F}_q^* , available online: <http://arxiv.org/pdf/1310.0776v2.pdf>.
- [27] M. Zieve, On some permutation polynomials over \mathbb{F}_q of the form $x^r h(x^{(q-1)/d})$, Proc. Amer. Math. Soc. 137 (2009), pp. 2209-2216.